Solution Brief

BROADCOM
MAINFRAME SOFTWARE

How Can Data-Centric Security Solutions Protect Data Privacy and Simplify Regulatory Compliance?

Challenge

The mainframe is mission-essential in the application economy and hosts the majority of the world's corporate data. With the immense amount of data on the platform, locating sensitive and regulated data, performing manual audits, and responding to potential security threats can be more than time consuming, it can seem impossible.

Opportunity

Data-centric mainframe security and compliance solutions, Data Content Discovery and Compliance Event Manager find sensitive and regulated data, classify data for compliance, alert you to potential risks in real time, and inspect threats through advanced reporting and forensics. This powerful combination can help you secure sensitive information across all aspects of the data lifecycle, facilitate regulatory compliance, and proactively address malicious attacks and the impacts of errors.

Benefits

The solution augments traditional user access management with data-centric compliance. It provides the only sensitive data discovery solution that runs 100% on the mainframe. By integrating data security and compliance management on the mainframe, you gain a deeper insight into security and compliance issues, and an improved risk posture. The result is that you can identify and locate your sensitive and regulated mainframe data, when it moves, and who has access to it.

Data-centric mainframe security and compliance solutions, Data Content Discovery and Compliance Event Manager identify sensitive data at rest and in motion to help lower the risk of damaging data breaches and to reduce the ongoing cost of regulatory compliance.

You Cannot Protect Your Sensitive Data If You Do Not Know Where It Is

The mainframe is essential and hosts the majority of today's enterprise data, which is also the majority of the world's most sensitive data. These huge aggregations and collections of regulated data can get lost, abandoned, orphaned or even maliciously hidden by internal fraudsters, subjecting enterprises to unknown degrees of risk.

With the vast amount of data residing on the mainframe, locating sensitive and regulated data to implement security controls and facilitate regulatory compliance can be more than time-consuming, it can seem impossible. You must know where your sensitive data is and who has access to it; and you must be able to act fast before your sensitive business data accidentally or maliciously exits the mainframe due to a data breach.

And now, the mainframe is increasingly connected with everything else in your business. While the connected mainframe drives significant business value, the number of risks increase, as well. The Internet, Internet of Things (IoT) and millions of mobile devices are now connected through APIs, causing mainframe data to grow, to move on and off the platform, and to become increasingly regulated. An enterprise-wide data-centric security strategy is critical to managing today's risk.

A Data-Centric Approach to Mainframe Security and Compliance

Enterprises are forced to accelerate their business and digital transformation due to changing competitive landscapes and continually evolving regulations. Adapting to new technology and services is inevitable, and these changes introduces additional risk and regulatory compliance requirements for the data. This puts organizations in a difficult position to guarantee that customer data is secure and private or to prove to auditors that controls are in place to fulfill regulatory compliance. To improve your risk and compliance posture, market leader Broadcom offers Data Content Discovery and Compliance Event Manager for the mainframe platform and a suite of Data Loss Prevention solutions for endpoints, servers, storage, network, email, and cloud.

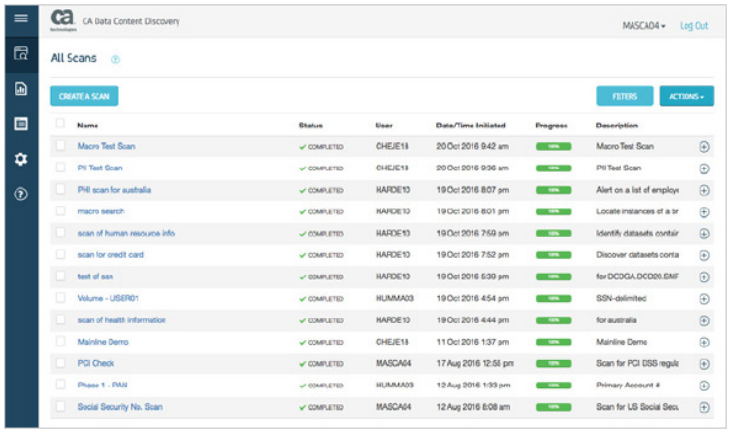
A Data-Centric Approach to Mainframe Security and Compliance (cont.)

Consider the following actions:

- **Start with the data:** The first step is knowing where your sensitive data resides on the mainframe. After all, if you cannot locate the data, how can you possibly know who is accessing it and how? You must find where your crucial data is stored, identify the data type and its sensitivity, understand the risk it faces, and manage how it is handled to enhance data privacy.
- **Understand which data is under threat:** After you have identified the location of your data, consider the type and amount of data, its nature, and its exposure to risk, so that you can determine your organization's risk posture. It is also important to determine how much of the data is subject to regulatory compliance.
- **Monitor access to that data:** Once a data set is identified as sensitive, it is critical to know who is accessing the data, when they are accessing it, and whether their access deviates from their normal activity so that you avoid misuse by putting the appropriate user controls in place.
- **Limit access to that data:** Once data has been identified as sensitive, determine who is accessing that data and, critically, who has accessed that data in the past. Ask yourself, do all of these users regularly access the data? Those who rarely access it are prime candidates for revocation, which is an easy start to implementing least access principles, leading to more control over your corporate business data.

Enterprises without confidence in the classification of their mainframe data typically have too many users allowed access to sensitive data, which leaves the business at high risk of data compromise from credential theft and insider threat, both unintentional and fraudulent.

Figure 1: Data Content Discovery



Our data-centric approach to mainframe security and compliance starts from the inside out. The first step is to identify and classify data on the mainframe, which allows you to examine which users have access to data and to reduce that access to only those who have a business case.

The second step is to monitor user access and alerts in real time. Real time monitoring gives you the power to act quickly, if necessary. For instance, real-time monitoring that shows frequent access to data or frequent movement of data by a user could help you to identify a potential insider threat before it happens.

Find, Classify, and Protect with Data Content Discovery

Data Content Discovery is the only data security discovery and classification solution that executes solely on and for the mainframe to eliminate the risk of offboarding sensitive data. The solution integrates with leading access control products such as ACF2™, IBM RACF and Top Secret®, revealing not just which data is exposed but also who has access to it, for both data at rest and data in motion.

Data Content Discovery finds sensitive data that might be lost, hidden, or abandoned. The solution then classifies the data based on its sensitivity level. Classifying the data by sensitivity level helps to facilitate regulatory compliance and to protect your most sensitive corporate data, the first steps in a data-centric approach to mainframe security.

"The most valuable feature of Data Content Discovery is the ability to recognize, in an intelligent and accessible way, which data sets on the mainframe contain sensitive data that needs to be protected from a governance and regulatory perspective."

Find, Classify, and Protect with Data Content Discovery (cont.)

Find

Data Content Discovery automatically scans the mainframe data infrastructure to immediately identify the location of sensitive and regulated data. Identifying the location of the data is the key to mitigating the risk that is associated with the retention of data.

Once you know the location, you can make business decisions to appropriately secure, encrypt, archive, or delete the data.

Data Content Discovery supports file types that span physical sequential, PDS/PDSE, VSAM, DB2, USS, and IMS (SHISAM, Datacom® and IDMS), covering all core mainframe applications. And the solution's support for data-in-motion helps prevent the costly loss of sensitive data that is moving on the platform.

Classify

Once Data Content Discovery finds the location of sensitive and regulated data, the software classifies the discovered data based on its sensitivity level so that you can place the appropriate safeguards around the data.

With the growing urgency to comply with industry regulations such as the European Union General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX), the need to quickly communicate your compliance posture to auditors is more critical than ever. Data Content Discovery enables you to prove to your auditors that controls are in place. Further, you can demonstrate that you are checking data by type and content and monitoring where data is being accessed on the mainframe.

Protect

Data Content Discovery helps key stakeholders stay in control of their corporate data, gain quick and critical insights about the potential and magnitude of data exposure from the mainframe, act quickly and reduce risk, all while reducing the costs associated with data protection processes. By identifying data exposure risks, classifying the data to determine its sensitivity level, and providing comprehensive reporting on the scan results, you can protect data, address compliance requirements, and mitigate exposure risks.

Alert, Inspect, and Protect with Compliance Event Manager

Running 100% on the mainframe, Compliance Event Manager helps mitigate data breaches and insider threats through real-time alerting and advanced reporting. The software provides immediate insights about the magnitude of data exposure on the mainframe, comprehensive auditing and forensics support to inspect compliance issues. These deeper insights help to protect mission-essential assets, eliminate risk, and reduce the cost of data protection processes.

Alert

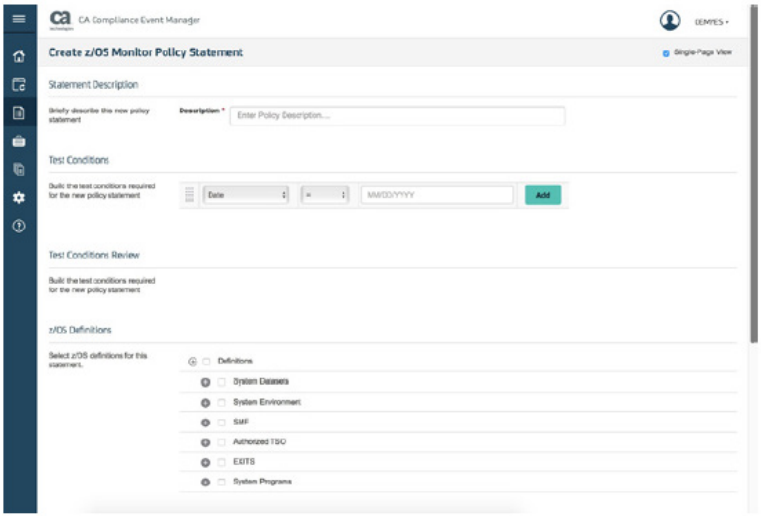
Compliance Event Manager helps to mitigate negative security events by alerting on potential risks in real time. The solution monitors entire systems of security records, security configuration points, system data sets, and IBM z/OS configuration controls. The solution provides immediate notifications of pertinent violations, plus access and change activities to critical security systems and resources.

Alerts to potential risk as they occur enable you to gain immediate and critical insight about the potential and magnitude of data exposure on the mainframe so you can act proactively in its remediation and improve your data privacy.

Inspect

Once data exposure threats are identified, Compliance Event Manager generates audit and compliance information, through comprehensive auditing and forensics support, that is not available in standard security reports. The software enables users to create real-time security alerts, supports forensic analysis of security situations with raw security data recording, and provides the ability to search, filter, archive and analyze recorded historical data.

Figure 2: Compliance Event Manager



Alert, Inspect, and Protect with Compliance Event Manager (cont.)

Additionally, Compliance Event Manager provides enterprise wide insights through an export of mainframe security incidents to Splunk, including a Compliance Event Manager Splunk application. This integration with Splunk provides a single-pane-of-glass view of risks that enables security and audit professionals to better manage end-to-end security in an enterprise.

Protect

Compliance Event Manager is designed to make regulatory compliance faster and easier by helping you to mitigate negative security events. The solution also helps you to address and reduce the total cost of compliance to keep your mission-essential data secure, and to lower risk. The solution provides deeper insight into data security and compliance, enabling you to locate data when it moves and to determine who has access to it.

Enterprise-Wide Data Centric Security and Compliance

Data Content Discovery and Compliance Event Manager simplify security management across the enterprise and enable robust, end-to-end protection for data in motion from mobile to the mainframe. These two solutions are the only data-loss prevention solutions in the market that run 100% on and for the mainframe and include all core mainframe applications, with simpler reporting and coverage.

Compliance Event Manager is designed to make regulatory compliance faster and easier by helping you to mitigate negative security events. The solution also helps you to address and reduce the total cost of compliance to keep your mission-essential data secure, and to lower risk. The solution provides deeper insight into data security and compliance, enabling you to locate data when it moves and to determine who has access to it.

Data Content Discovery and Compliance Event Manager simplify security management across the enterprise and enable robust, end-to-end protection for data in motion from mobile to the mainframe. These two solutions are the only data-loss prevention solutions in the market that run 100% on and for the mainframe and include all core mainframe applications, with simpler reporting and coverage.

As the IT workforce trends toward a younger, experience-hungry demographic, Broadcom® data security solutions provide a simplified yet thorough dashboard that gives IT teams of any skill level the visibility to see and respond to potential vulnerabilities across the enterprise.

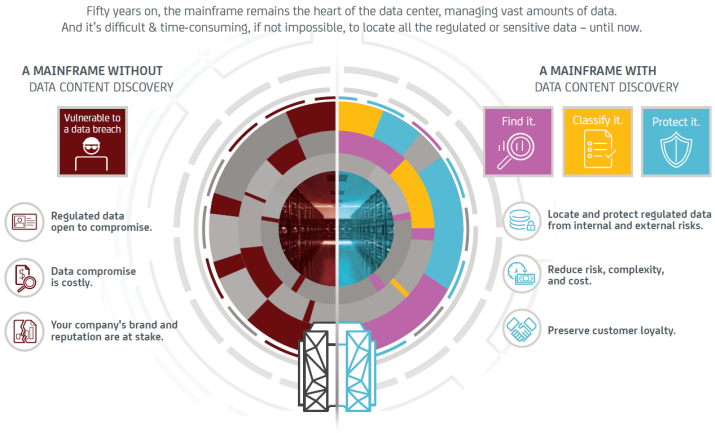
Broadcom data security solutions also enable you to adapt as the mainframe continues to evolve. The mainframe transacts the majority of enterprise data, plays a critical role in the increasing volume and velocity of mobile and IoT transactions, and is pivotal to new regulations, such as the EU-U.S. Privacy Shield agreement and the GDPR.

Broadcom data security solutions eliminate the need for manual audits because they quickly isolate sensitive data, which is the first step in GDPR data privacy compliance.

From finding and classifying, to alerting and inspecting, Data Content Discovery and Compliance Event Manager provide unified enterprise security while helping to increase compliance posture across all platforms.

For more information, please visit our site: mainframe.broadcom.com/security

Figure 3: Why Data Content Discovery?



BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

CS200-284062-0322 March 29, 2022